モバイル端末における多重インタラクティブ個人認証システムの提案

長谷 容子　　青木 輝勝　　安田 浩

東京大学大学院 工学系研究科

{yohko, aoki, yasuda}@mpeg.rcast.u-tokyo.ac.jp

本稿では、モバイル端末を利用した多重インタラクティブ個人認証システムを提案する。本システムを用いれば、EC 等のアプリケーション・サービス側とそのサービスを利用するモバイル端末ユーザーとの間のやりとりを通して、ユーザーの現在おかれている環境や利用しようとするアプリケーションの必要とするセキュリティ・レベルに応じた適切な認証手法を選択し、適用することができる。また、複数の認証手法を組合わせて、トータルとしての認証精度を確保するように設定することも可能であり、モバイル端末という特性を積極的に利用した新しい認証手法のさまざまな実現が可能となる。本稿の最後では、具体的に本システムを適用した認証の例について示す。

キーワード：モバイル端末、多重個人認証、インタラクティブ認証

A Proposal of Multi Interactive Person Authentication System Using Mobile Phone

Yohko Hase　　Terumasa Aoki　　Hiroshi Yasuda

Research Center for Advanced Science and Technology, the University of Tokyo

In this paper, we propose a multi interactive person authentication system using mobile phone. This system makes it possible to select suitable person authentication methods and to apply them to application services according to the user’s conditions and security level of the applications. We describe the subsystems and the main functions that construct the whole system. In the last of this paper, we also show concrete examples of the system to authenticate the users using their biometorics data, location data, and schedule data.

Keyword: Mobile Phone, Multi Person Authentication, Interactive Authentication

１．はじめに

インターネットの急激な発展により、情報ネットワーク・インフラは、従来の「便利さが優先されるフェーズ」から「社会のインフラとしての信頼性を前提とするフェーズ」に移行してきている。個人認証技術は、その信頼性を支える最も重要な技術の一つであり、これまでにもさまざまな研究がなされてきた。例えば、個人認証の方法として、「パスワード等の個人が持つ秘密情報を利用したもの」、「IC カード等の個人所有物を利用したもの」、「指紋等の個人固有の身体的特徴を利用したもの（バイオメトリクス）」、「手指動等の個人の行動特性を利用したもの」[1] 等の検討が盛んにおこなわれている。しかしながら、従来の研究の多くは、それぞれの個別の手法における認証精度を向上させることを主眼にしたものが多く、実際にネットワークを利用したアプリケーション・サービスを提供するシステムの一部として位置付けられる個人認証技術という視点から必要とされる機能や手法については、あまり検討されていない。

また、従来のデスクトップ・パソコン等の固定設置タイプの端末に代わって、携帯電話をはじめとするモバイル端末の普及が進み、文字通り“ いつでも ”“ どこでも ”インターネット・バンキングやインターネット・ショッピング等をおこなうことができるようになったが、こうしたアプリケーション・サービスを利用する利用者が使う端末の特徴を考慮

した視点に基づく認証システムに関する検討も、まだ、ほとんどなされていない。

そこで本稿では、モバイル端末を利用する場合を想定した新しい個人認証システムとして、“モバイル端末における多重インタラクティブ個人認証システム”を提案する。

まず、第 2 章で、従来の個人認証技術の課題と解決の方向性について整理する。続く第 3 章では、モバイル端末を用いた個人認証に求められる要件をまとめ、それらの要件を満たす一つの具体的なシステム・イメージとして、「モバイル端末における多重インタラクティブ個人認証システム」を提案し、その主な機能について述べる。また、具体的な適用例についても紹介する。最後に第 4 章で、まとめと今後の課題について簡単に述べる。

2．従来の個人認証技術における課題と解決の方向性

2．1 従来の個人認証技術と課題

従来の個人認証技術は、以下のように、大きく3つのカテゴリーに分けることができる。

（1）秘密情報による認証

パスワード認証に代表されるように、その個人のみが知っている知識の照合に基づく認証であり、特別な装置を必要としないため、現在、最も広く普及している方法と言える。しかしながら、秘密にする情報が簡単なもの（短いパスワード等）であると、破られる可能性が高く、複雑なもの（長いパスワード等）であると利便性が著しく低下するという特徴を持つ。

（2）所有物による認証

ID カードによる認証に代表されるように、その個人のみが所有している物を照合することによる認証であり、耐改ざん性に優れた安価なものが出現したことにより、普及の傾向にあるが、常に、携行しなくてはならないという利便性の低さがある。

（3）バイオメトリクスによる認証

その個人しか持ち得ない身体的特徴（指紋、掌形、静脈パターン、耳介、虹彩、網膜、DNA 等）や行動的特性（署名、声紋等）を照合することによる認証であり、究極の本人確認の方法と言われるが、パターン認識技術等の照合技術やデータを取得するセンサーの精度等の限界から、認証精度を 100%にすることができない。また、身体的特徴は、基本的に不変であるため、もし、仮にデータが盗まれることが生じても、データの更新や変更はできない。

2．2 課題のまとめと解決の方向性

これらの各個人認証技術における共通した課題として、以下のことをあげることができる。

- 各認証技術ごとに、その特徴ゆえに 100%解決することが困難であるという本質的な課題が存在している。
- 常に単一の認証方法だけでは、悪意を持った第三者等によって集中的な攻撃を受ける可能性が高く、破られる危険性が増す。また、実際に破られた場合のシステム全体への影響が大きい。
- 各認証方法において、付加的なハードウェア装置や設備等を併用することによって、セキュリティ・レベルを上げることが期待できるが、利便性は低下してしまうことになる。

本稿では、モバイル端末を利用した個人認証を考えるにあたり、これらの課題を解決するために、大きく2つの方向性をあげる。

（1） トータルとしての認証精度やセキュリティ・レベルに配慮し、認証の方法や回数を複数にする。

バイオメトリクスを組合せて認証する方法は既に議論されているが [2]、ここではバイオメトリクスだけに限らないで考えることにする。

（2） モバイル端末が持つ特徴を考慮する。

従来の固定端末（デスクトップ PC 等）にはなかった利便性や機能性を生かすとともに、弱点を補う配慮をする。

３．モバイル端末における多重インタラクティブ個人認証システム

３．１ モバイル端末における個人認証に求められるシステムの要件

課題解決の方向性をより具体的にして、モバイル端末における個人認証に求められるシステムの要件を導くために、携帯電話やＰＤＡ等のモバイル端末をクライアントとする際のサービス利用者側の特徴を整理すると、以下のようになる。

＜特徴-Ｍ１＞標準で搭載されている機能の多様化

例えば、最近の携帯電話を想定して、入力に関するユーザー・インターフェースを考えると、ボタン式の数字キーボードの他に、十字型のキーやダイヤル式のキーによる入力が可能であったり、マイクによる音声の入力だけでなく、搭載されている小型カメラによる画像の入力（撮影）ができるものが登場している。また、指紋センサーの搭載も可能となってきている。更に、入力以外の機能としても、ＧＰＳ（Global Positioning System）機能や着信時のマナーモードとして利用されている振動機能等、標準として搭載されている機能は非常に多様化してきていると言える。これらの機能を認証の際にも利用することが可能である。

＜特徴-Ｍ２＞不特定な利用環境・場所

モバイル端末は、その名の通り、持ち歩くための端末であり、利用する環境や場所はさまざまである。このことは、設置場所が固定されているデスクトップ・パソコンを利用する場合と比べて、利用者の端末を利用する環境や場所にともなう条件が、利用の度に異なる可能性が高いことを意味している。この本質的な特徴を考慮して、認証方法を考えることが必要である。

＜特徴-Ｍ３＞小型・軽量化が本質的

持ち歩くというモバイル端末の本来の目的を考えると、当然ながら端末の形態は、より小型で軽量なものが好まれて普及している。ある程度の設置スペースが前提とされるデスクトップ・パソコン等と比較すると、利用者がモバイル端末を選択する際に、この特徴は、かなり重視されるものの一つと考えられる。そのため、認証方法の普及を考える際には、そうした利用者の好みや利便性を損なわない配慮も必要である。

アプリケーション・サービス側の特徴としては、以下の事項が上げられる。

＜特徴-Ａ１＞認証方法が一つに限定されている場合のリスクの増加

アプリケーション・サービスが要求する認証方法がいつも同一である場合、一般に、ハッカー等に狙われ、破られるリスクが大きいと考えられる。そのため、アプリケーション・サービス側では、できるだけ多様な認証方法の利用を可能にし、リスクの分散をはかることが必要である。

＜特徴-Ａ２＞アプリケーションごとに異なるセキュリティ・レベル

例えば、数百円の商品を販売するＥＣアプリケーションと、数万～数十万円の商品を販売するＥＣアプリケーションでは、必要となるセキュリティ・レベルは異なると考えられる。名前だけを登録することによって利用できるアプリケーションと、クレジット番号等の機密性の高い情報や病歴等のかなりプライバシーの高い情報を登録しないと利用できないアプリケーションについても、やはり要求されるセキュリティ・レベルは異なる。一般に、セキュリティ・レベルが高い認証方法が求められることは当然であるが、実際の運用を考える上では、＜特徴-Ｍ３＞で述べた利用者の利便性とのバランスも考慮し、アプリケーションに応じたセキュリティ・レベルの認証方法を選択できることが望ましいと言える。特に、複数のアプリケーション・サービスを提供するポータルサイト等においては、考慮すべき特徴の一つであると言える。

＜特徴-Ａ３＞一回きりの認証判定結果に依存することによるリスクの増加

ネットワークを利用したアプリケーション・サービスであるために、直接本人と対面して本人認証をおこなうことができないことによるリスクは、避けられない。特に、設置場所に関するセキュリティを配慮することが可能なデスクトップ・パソコン等をクライアントが利用する場合と比べて、モバイル端末では紛失したりするリスクや、＜特徴-Ｍ２＞で述べた不特定な利用環境や場所によって認証の精度が影響を受ける可能性のリスクが生じる。そのため、一回きりのやりとりによって認証判定を下すよりも、複数回のやりとりを利用して、最終的な認証判定を導くことがリスクの軽減において有効である。

これらの特徴から、モバイル端末を用いた個人認証において、以下のようにシステムの要件をあげることができる。（図１）

（１）サービス利用者側において、認証に用いる特徴量の入力方法の多様化をはかる。

（２）サービス利用者側において、利用する環境に応じた最適な認証方法の選択を可能にする。

（３）サービス利用者側において、携帯することによる利便性を考慮する。

（４）アプリケーション・サービス側において、認証のために要求する特徴量の多様化をはかる

（５）アプリケーションの必要とするセキュリティ・レベルに応じた認証方法の適用を可能にする。

（６）サービス利用者とアプリケーション・サービス側の間において、複数回のやりとりを可能にし、認証方法や認証判定の多様化をはかる。

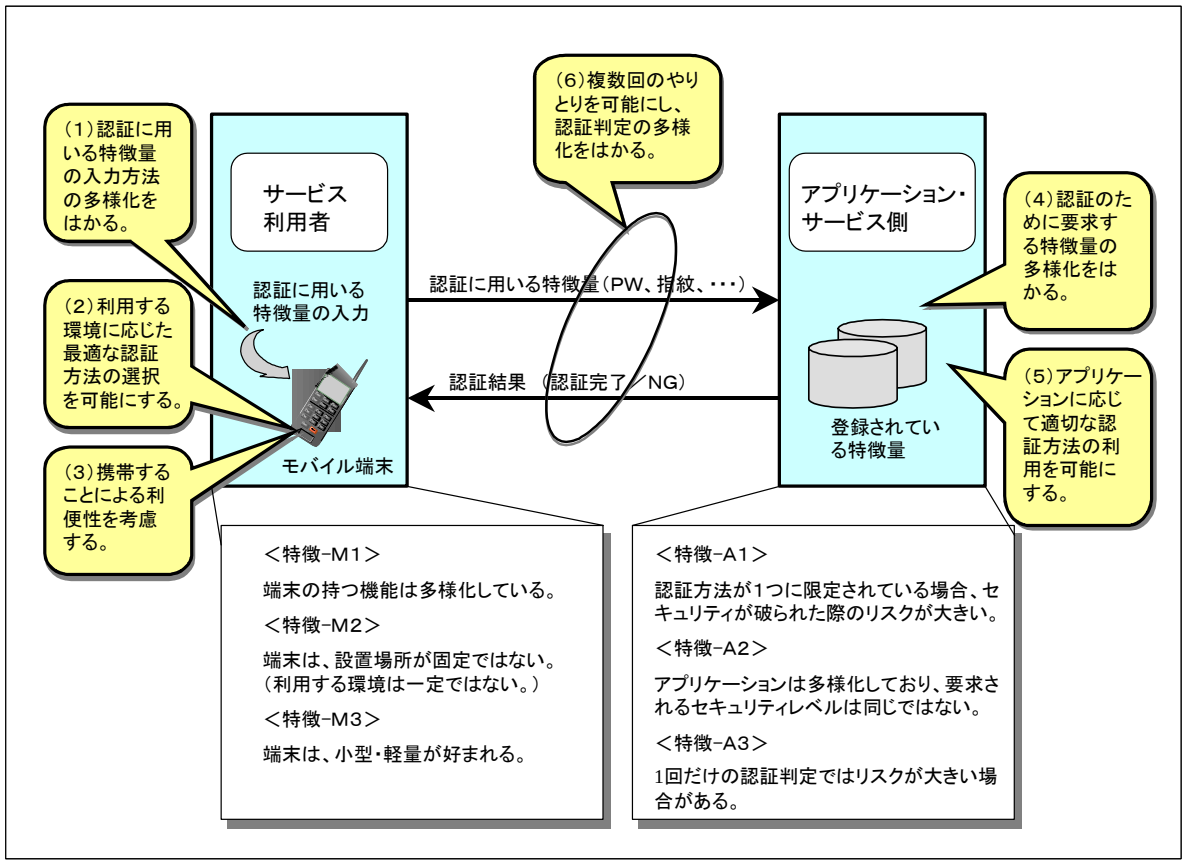

図１　サービス利用者とアプリケーション・サービス間のやりとりにおける個人認証に関する要件

３．２ モバイル端末における多重インタラクティブ個人認証システムの概要

前節で上げた要件を満たす一つの具体的なシステム・イメージとして、本稿では、モバイル端末における多重インタラクティブ個人認証システム（図２）を提案する。本システムは、以下のようなサブシステムと機能から構成される。

＜認証インフラ・システム（アプリケーション・サービス側）＞

（Ｓ１）認証手法パレット・サブシステム

アプリケーション・サービス側において、以下のような複数の認証手法に関連する機能を可能にするサブシステムである。

① パスワード認証機能
パスワードによる認証を可能にするもので、利用者のパスワードが登録されている DB と連携して機能する。

② PKI 認証機能
PKI による認証を可能にするもので、利用者のデジタル証明書が登録されている DB と連携して機能する。

③ バイオメトリクス認証機能
バイオメトリクスによる認証を可能にするもので、利用者の指紋データや声紋データ等のバイオメトリクスデータが登録されている DB と連携して機能する。

この他に、行動特性を利用した認証手法等、複数の認証手法を登録することができる。

（Ｓ２）認証手法設定サブシステム

アプリケーション・サービス側において、アプリケーションやサービス利用者に応じて、適切な認証手法の適用を判断するもので、（Ｓ１）で記述した認証手法パレット・サブシステムで登録されている複数の認証手法を単独、あるいは、組み合わせて利用することを可能にするサブシステムであり、主に以下の４つの機能から構成される。

① アプリケーション・セキュリティ・レベル管理機能
アプリケーションごとに必要とされるセキュリティ・レベルを設定し、管理することを可能にするもので、それぞれのレベルに対応した認証精度やそれらの認証精度を実現するための認証手法を適切に判断し、サービス利用者へ適用するための機能である。

② クライアント認証環境判定機能
後述するサービス利用者側のサブシステムの機能であるクライアント入力サブシステムの利用者環境入力機能（（Ｃ１）①）によって入力されたサービス利用者のおかれている現在の環境条件（「雑踏の中にいる」、「湿度の高い場所にいる」等）を受けて、その状況に適した認証精度や対応する手法を判断する機能である。

③ 認証精度設定機能
アプリケーション・セキュリティ・レベル管理機能（（Ｓ２）①）やクライアント認証環境判定機能（（Ｓ２）②）における結果を受けて、適切な認証精度を判断して設定する機能である。

④ 認証手法組合せ設定機能
認証精度設定機能（（Ｓ２）③）を受けて、適切な単独の認証手法、あるいは、複数の認証手法を選択して設定する機能である。

（Ｓ３）認証結果判定サブシステム

アプリケーション・サービス側における機能であり、アプリケーション・サービス側が指定した認証手法に対して、サービス利用者が入力した認証データ（特徴量）を受けとり、認証の結果を判定するサブシステムであり、主に以下の２つの機能から構成される。

① 個別認証結果判定機能
適用した認証手法ごとに、認証結果を判定する機能であり、単独の認証手法のみを適用した場合には、その一つの結果をトータル認証結果判定機能（（Ｓ３）②）に引き

渡し、複数の認証手法を組合せて適用している場合には、それぞれの認証手法ごと生じた複数の個別の結果をトータル認証結果判定機能（（Ｓ３）②）に引き渡す。

② トータル認証結果判定機能
個別認証結果判定機能（（Ｓ３）①）から受け取った認証結果に基づき、単独の認証手法のみを適用した場合には、その結果そのものをサービス利用者へ返信し、複数の認証手法を組合せて適用している場合には、組合せを構成している個々の認証手法のそれぞれの結果を統合して最終的な認証結果を判定し、サービス利用者へその結果を返信する機能である。

＜認証インフラ・システム（サービス利用者側）＞

（Ｃ１）クライアント入力サブシステム

サービス利用者側において、認証に関連したデータの入力を可能にするサブシステムであり、主に以下の２つの機能から構成される。

① 利用者環境入力機能
認証を受けようとするサービス利用者が、必要に応じて、自分の置かれている場所や環境に関するデータを入力することを可能にする機能であり、入力結果は、アプリケーション・サービス側のサブシステムの機能である認証手法設定サブシステムのクライアント認証環境判定機能（（Ｓ２）②）に引き渡される。

② 利用者認証申請機能
認証を受けようとするサービス利用者が、アプリケーション・サービス側から要求された認証データ（特徴量）を入力し、認証判定を申請する機能であり、入力結果は、アプリケーション・サービス側のサブシステムの機能である認証結果判定サブシステムの個別認証結果判定機能（（Ｓ３）①）に引き渡される。

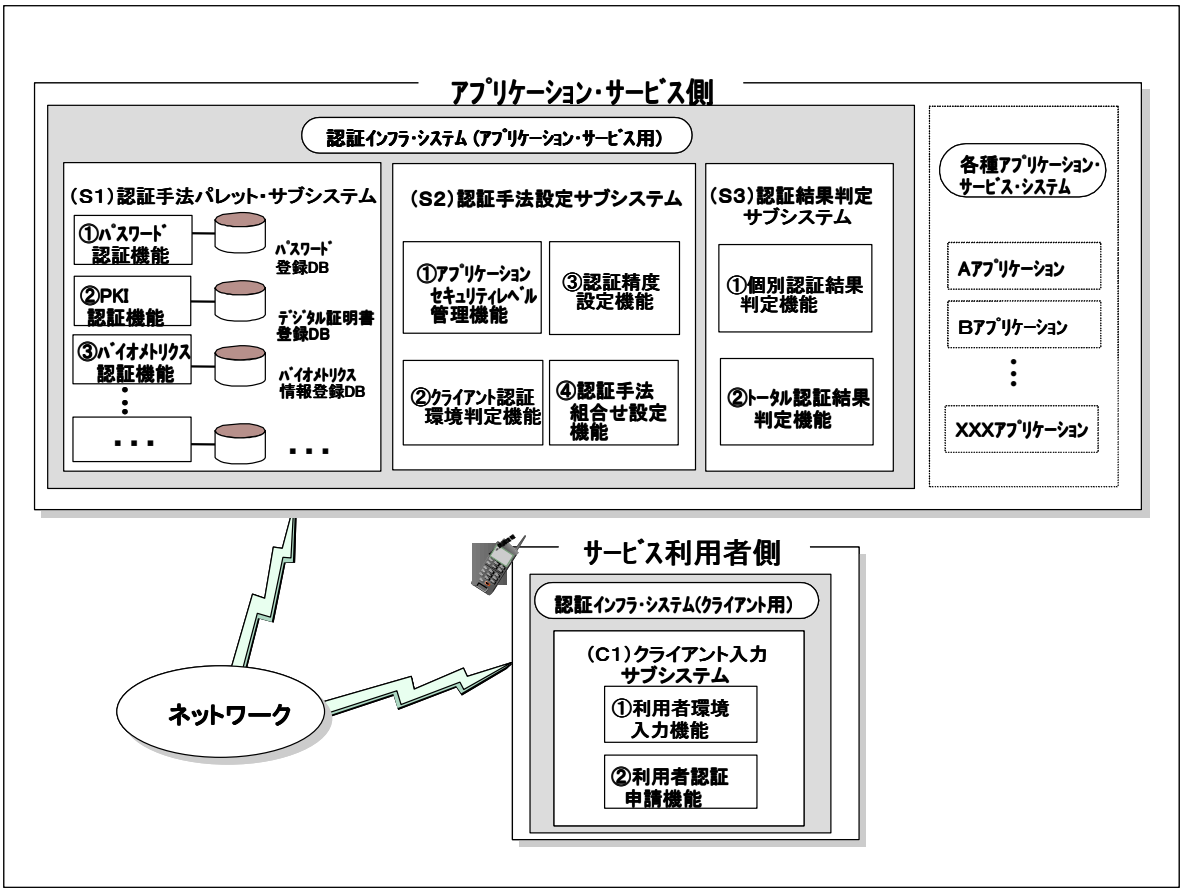

図２　モバイル端末における多重インタラクティブ個人認証システム

３．３ 具体的な適用の例

本節では、前節で述べたシステムを具体的に適用した認証の例を示す。

＜例１：サービス利用者が、雑踏の中で携帯電話を利用した個人認証をおこなう場合。＞

サービス利用者が、「自分が現在雑踏の中にいること」、及び、「利用したいアプリケーション名」をアプリケーション・サービスサイトへ伝えることにより、アプリケーション・サービス側で、その特定のアプリケーションに要求されるセキュリティ・レベルを判断し、そのレベルに対応した認証精度や認証手法の組合せを設定して、サービス利用者に指示する。認証手法の組合せとして、「指紋認証」と「耳の画像による認証」を選択した例を図３に示す。

＜例２：サービス利用者が、あらかじめ予定していた特定の場所において、携帯電話を利用した個人認証をおこなう場合。＞

サービス利用者が、「自分があらかじめ予定していた特定の場所にいること」、及び、「利用したいアプリケーション名」をアプリケーション・サービスサイトへ伝えることにより、アプリケーション・サービス側で、その特定のアプリケーションに要求されるセキュリティ・レベルを判断し、そのレベルに対応した認証精度や認証手法の組合せを設定して、サービス利用者に指示する。認証手法の組合せとして、「ＧＰＳの値、スケジュールデータ、特定の場所における画像データの照合によって認証」する方法を選択した例を図４に示す。

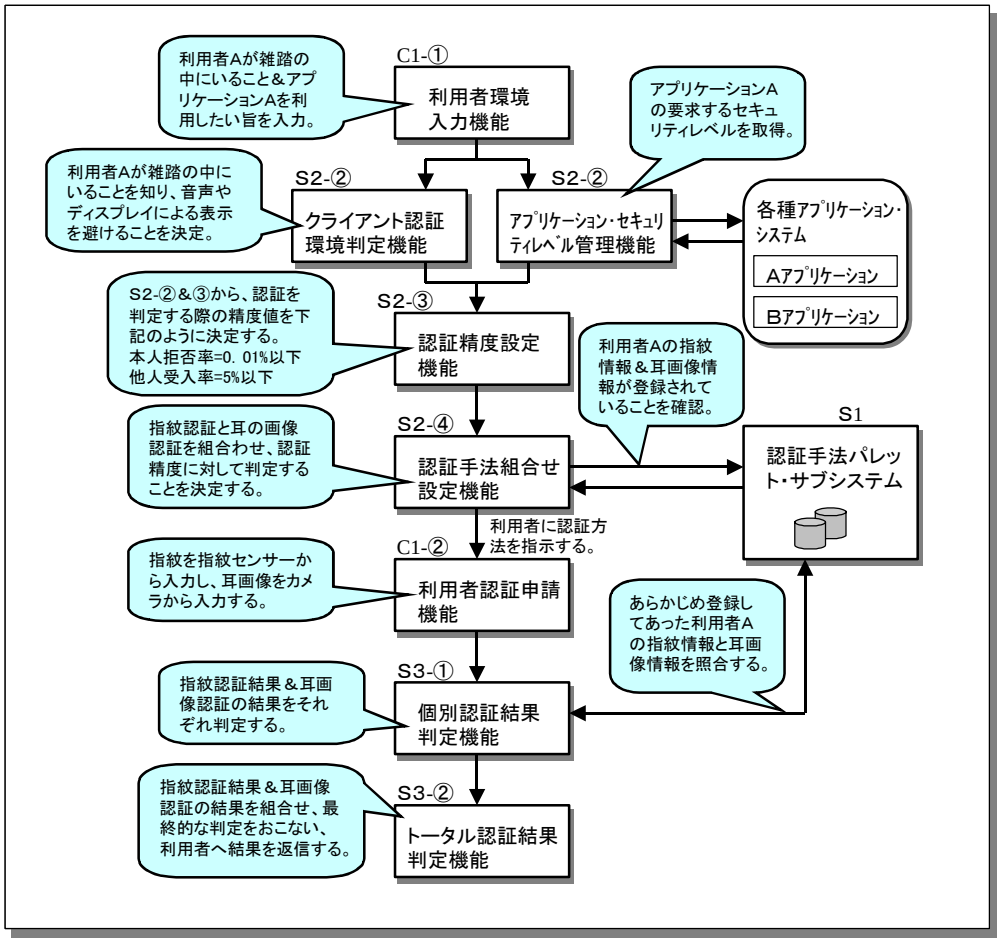

図３ サービス利用者が、雑踏の中で、携帯電話を利用した個人認証をおこなう場合の例

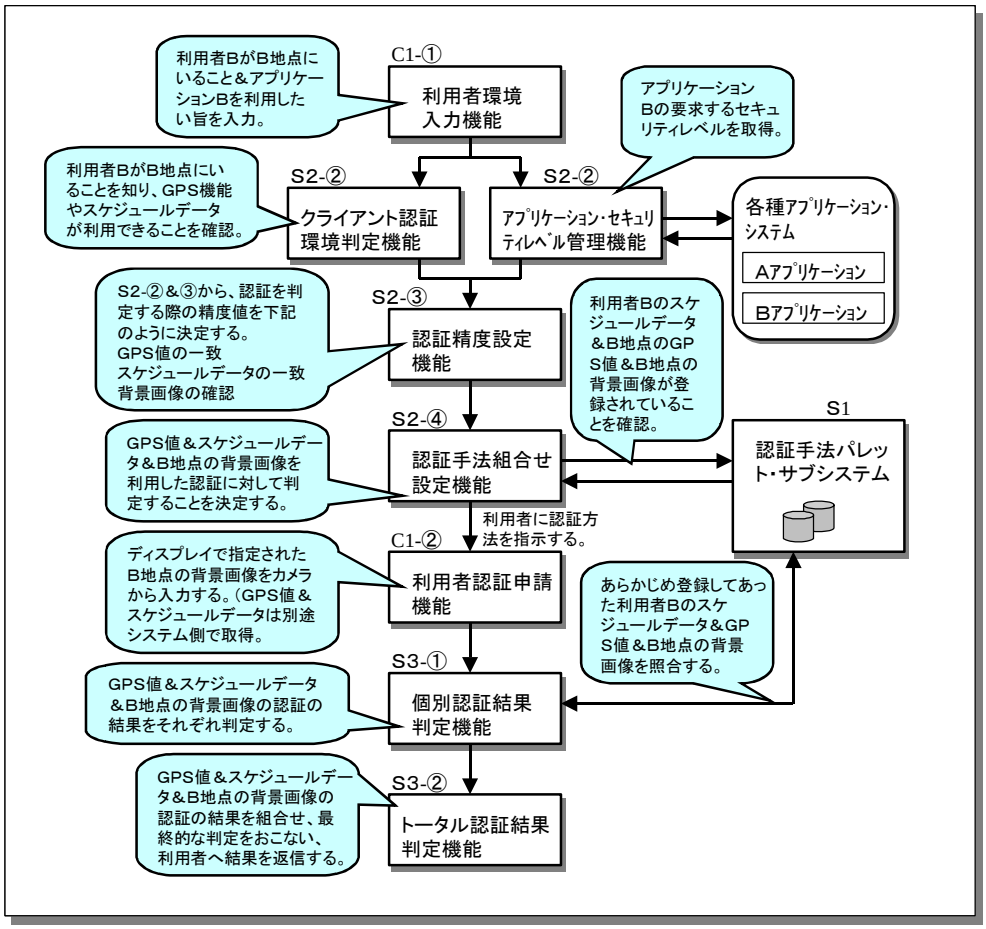

図４　サービス利用者が、あらかじめ予定していた特定の場所において、携帯電話を利用した個人認証をおこなう場合の例

４．まとめ

本稿では、モバイル端末を利用して個人認証をおこなう際に考慮すべき要件を検討し、一つの具体的なシステム・イメージとして、「モバイル端末における多重インタラクティブ個人認証システム」を提案し、実際に適用した認証の例を示した。

本システムによれば、認証手法の組合せによる効果だけでなく、モバイル端末という特性を積極的に利用した新しい認証手法のさまざまな実現が可能となる。

今後は、「安全性」、「利便性」、「経済性」、「社会的受容性」等の視点から評価実験をおこない、本システムの有効性を更に検討していきたい。

参考文献

[1]　長田礼子，尾崎哲，青木輝勝，安田浩，“手指動からの特徴抽出によるリアルタイム個人認証“，電子情報通信学会論文誌 D-II, Vol.J84-D-II, No.2, pp.258-265, 2001.

[2]　坂野鋭，“バイオメトリクス個人認証技術の動向と課題“，信学技法，PRMU99-29,pp.75-82,June 1999.

[3]　長谷容子，青木輝勝，安田浩，“多重インタラクティブ個人認証システムの提案”電子情報通信学会 2002 年総合大会 A-7-14, 2002.